INTELLECTUAL PROPERTY - BRING YOUR OWN DEVICE

CT
(REGULATION)

OVERVIEW

Many Staff and Students have personal hardware devices, software applications, utilities, tools, software development kits, and related products that do not meet College of the Mainland's security requirements.

PURPOSE

The purpose of this Regulation is to establish the rules for the use of Staff and Student owned devices and technologies that utilize and access College of the Mainland Information Resources.

SCOPE

This Regulation applies to all College of the Mainland Staff and Students that utilize Staff owned devices and technologies that utilize and access College of the Mainland Information Resources.

REGULATION

While College of the Mainland has a Bring Your Own Device (BYOD) culture, risks related to these devices must be managed.

On an annual basis the IT Department shall survey College of the Mainland Staff about devices, operating systems, applications, browsers, tools, utilities, scripts, software development kits, cloud services, and related technologies used. The IT Department shall perform a BYOD analysis to determine:

- If the devices and/or technologies used pose a risk to College of the Mainland's Information Systems.
- Changes or configurations necessary to minimize risks to College of the Mainland's Information Resources.
- Mandatory security components (e.g. firewall, anti-malware protection, passwords, browser security settings, patch management, encryption, physical controls) needed as a condition for allowing BYOD devices and technologies to access College of the Mainland Information Resources.
- Prohibited devices and technologies.
- Devices and technologies allowed to access College of the Mainland's Information Resources.
- Level of access (e.g. restricted, full, guest, admin) granted to the devices and technologies.

The IT Department shall implement controls that mitigate risks:

- The IT Department shall ensure Staff access to sensitive data from BYOD devices and technologies have strict password and encryption controls in place
- Anti-malware software shall be used and updated on a regular basis.

- In some instances, the IT Department may identify applications that, due to their sensitive nature, may not be accessed by BYOD devices and technologies.
- Limit activities performed on BYOD devices and technologies.
- The IT Department may restrict access to College of the Mainland Information Resources based upon a variety of factors.
- The IT Department will keep the Chief Information Officer (CIO) or his designee informed of BYOD threats so that the security awareness and training program can be updated.

In the event a device is lost or stolen, the IT Department shall quickly block access to Information Resources from the device. In addition, the IT Department shall:

- Wipe College of the Mainland data and applications, and/or
- Wipe the entire BYOD device if deemed necessary to ensure the security of College of the Mainland Information Resources. Wiping the entire BYOD device may have Staff and Student implications including the inability to make calls, loss of contacts, need to have the device restored, etc.

College of the Mainland shall not be held liable for the loss of use or restoring of device, operating system, software applications, tools, scripts, data, etc. Staff should take the proper precautions (e.g. physical controls over devices, backing up of contacts and files, etc.) to minimize any disruptions.

BYOD devices and technologies shall employ controls that meet the following requirements:

- Password required at start up (power on).
- Inactivity timeout.
- Password change frequency.
- Safeguards ensure only approved users of BYOD devices and technologies can access College of the Mainland Information Resources.

Staff and Students shall not:

- “Root” or “jailbreak” a BYOD device and technology to free it from pre-defined limitations. This process modifies the system files and can result in an unstable and insecure device.

- Modify BYOD device and technology hardware and/or software beyond installation of updates provided by the device maker or service provider.
- Disable BYOD device and technology protection systems including passwords, encryption, firewalls, and anti-malware without the approval of the IT Department.

The IT Department shall prepare a list of non-authorized BYOD devices and technologies that are not allowed to utilize and access College of the Mainland's Information Resources.

Staff shall be responsible for adhering to the requirements of this Regulation. Staff shall notify the IT Department when:

- A BYOD device is lost or stolen.

When choosing an appropriate plan, Staff and Students should consider the additional voice minutes and data traffic that may be incurred. College of the Mainland does not assume any financial responsibility for BYOD devices or technologies. College of the Mainland shall not reimburse Staff or Students for any expenses including but not limited to:

- BYOD device or technology initial cost, maintenance, or replacement
- Recurring costs related to voice and data usage, roaming, etc.
- Connectivity charges including Wi-Fi hotspots usage
- Insurance
- Expenses related to restoring BYOD devices or technologies if lost, corrupted (e.g. Malware, incompatible applications, changes to operating system), or damaged.

The College of the Mainland IT Department shall perform periodic risk assessments to identify, manage, and reduce BYOD device and technology related risks and access to Information Resources.

ENFORCEMENT

Any Staff found to have violated this Regulation may be subject to disciplinary action, up to and including termination.